Ollscoil na hÉireann, Gaillimh *GX_____*
National University of Ireland, Galway

Autumn Examinations, 2009

Exam Code(s)	4IF1
	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer security and forensic computing
Paper No.	1
External Examiner(s)	Prof. J.A. Keane
Internal Examiner(s)	Prof. G. Lyons
	Dr. C. Mulvihill
Instructions:	Answer any four questions.
	All questions carry equal marks.
Duration	3 hrs
No. of Answer Books	1
No. of Pages	1
Department(s)	Information Technology

1
An entrepreneur developing software for the bioengineering sector has secured funding and is setting up in the west of Ireland. You have been retained to provide initial advice on a security profile. Discuss elements of a report you might draft for this individual, making use of the following three headings: IP protection (8 marks), regulatory compliance (8 marks), audit trails (9 marks).

2
(a) What is your understanding of the term ‘steganography’? (6 marks)
(b) How does steganography differ from cryptography? (8 marks)
(c) Discuss any one technique employing steganography that would be suited to the following application: a short message to be transmitted composed of 100 or less characters (11 marks)

3 ‘Security is often concerned with confidentiality and integrity’
(a) Give a brief outline of two significant properties of the Bell-LaPadula model (8 marks)
(b) In commercial work, what is meant by the term ‘Chinese wall’? (8 marks)
(c) Briefly discuss two security implications of the electronic patient record (9 marks)

4
‘Cryptography may or may not be secure’
(a) Explain what is meant by the term ‘public key cryptography’ (6 marks)
(b) Discuss how a merchant might make use of public, private, and session keys in her dealings with customers, explaining the terms ‘digital certificate’ and ‘digital signature’ in the course of your answer (9 marks)
(c) You have access to a hard drive that is apparently encrypted. It is password protected. How might you approach the problem of accessing the contents of the laptop? (10 marks)

5
(a) Give your understanding of the term ‘phishing’ (7 marks)
(b) In your opinion why are phishing attacks effective? (8 marks)
(c) The FTC has linked phishing to identity theft. Why is identity theft a problem? (10 marks)

6
(a) Give your understanding of the ‘Daubert Criteria’ for scientific evidence (7 marks)
(b) Is it possible to conduct a full forensic examination of an iPhone in your view? (8 marks)
(c) Outline the steps that you would take in imaging a disk and searching it for content, explaining the terms ‘dd’ and ‘data carving’ in the course of your answer (10 marks)

7
‘The jury is still out on electronic voting’
Discuss this statement in the light of the relevant German Federal Constitutional Court decision in March 2009 (25 marks)